

**HIT Policy Committee
Privacy & Security Workgroup
Draft Transcript
May 7, 2010**

Presentation

Sarah Wattenberg – ONCHIT – Public Health Advisor

Thank you. Good afternoon. This is Sarah Wattenberg, staff to the privacy and security workgroup, and I'm filling in for Judy Sparrow today. I want to welcome everyone to today's Privacy & Security Workgroup call. As you may know, today's proceedings are open to the public. And, at the end of the call, the public will have the opportunity to make comments. I'd like to remind the members of the workgroup to identify themselves for our listening audience. And with that, I will turn it over to Deven McGraw.

Deven McGraw - Center for Democracy & Technology – Director

Great. Thank you, Sarah. You did an excellent job.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Why thank you. My debut.

Deven McGraw - Center for Democracy & Technology – Director

Your debut and Judy's shoes are incredibly big ones to fill, so you did an admirable job.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Why thank you.

Deven McGraw - Center for Democracy & Technology – Director

I think it would help though to take a roll call of the workgroup members to see who we have on the line, so can I ask you to do that since I don't have a list right in front of me? Thank you.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Absolutely. You know what? I do not have the list in front of me. That was not – so much for the debut. I will get the list momentarily. Hang on.

Deven McGraw - Center for Democracy & Technology – Director

That's okay. We're still in the very early part of the call.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Yes, we still have time.

Deven McGraw - Center for Democracy & Technology – Director

So that's okay.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Yes. I do have it here somewhere. I just pulled it. Okay. Let's take a roll call. Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

[Type text]

I'm here.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Anne Castro?

Deven McGraw - Center for Democracy & Technology – Director

Who is Anne Catherine?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

You know what? That's the privacy and security standards....

Sarah Wattenberg – ONCHIT – Public Health Advisor

That's the standards workgroup. Okay. This is one thing I wasn't told to do. Hang on.

Deven McGraw - Center for Democracy & Technology – Director

No problem.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Ironic.

Deven McGraw - Center for Democracy & Technology – Director

I notice that the first part of the agenda is introductions and overview of the agenda. I'll do the overview of the agenda, which is that we have one big thing to talk about.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Actually, you know, let's do it this way. Can we have members of the workgroup announce who they are?

Deven McGraw - Center for Democracy & Technology – Director

Sure.

Sarah Wattenberg – ONCHIT – Public Health Advisor

I think that's easier.

Deven McGraw - Center for Democracy & Technology – Director

Sure.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Sarah, this is Mike DeCarlo. Actually, I've got the list in front of me.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Thank you.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Would you like me to just go down it?

Sarah Wattenberg – ONCHIT – Public Health Advisor

Please do.

Deven McGraw - Center for Democracy & Technology – Director

Mike, thank you.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Thank you.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Deven McGraw?

Deven McGraw - Center for Democracy & Technology – Director

I'm here.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Rachel Block?

Deven McGraw - Center for Democracy & Technology – Director

Yes, I think Rachel is going to miss this call.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Paul Tang? Latanya Sweeney? Gayle Harrell? Mike Klag? Judy Faulkner? Paul Eggerman?

Paul Eggerman – eScription – CEO

Here.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Here.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Paul Uhrig? Terri Shaw? John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Here.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Joyce DuBow? John Blair? Peter Basch? Mike DeCarlo for Justine Handelman. Marianna Bledsoe?

Marianna Bledsoe – NIH – Deputy Associate Director

Here.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

David Wanser?

Dave Wanser – NDIIC – Executive Director

Here.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Kathleen Connor?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Here.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Jodi is not here, and Sarah Wattenberg.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Yes. Here.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

That's it.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Thank you.

Adam Green – Progressive Chain Campaign Committee – Cofounder

And this is Adam Green. I'm also on the line.

Deven McGraw - Center for Democracy & Technology – Director

Great. Thanks, Adam. Do we know if we have Joy on?

Sarah Wattenberg – ONCHIT – Public Health Advisor

It doesn't sound like it.

Ellen Flink – NYS DOH OHITT – Director Research, Patient Safety & Quality

Deven?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Ellen Flink – NYS DOH OHITT – Director Research, Patient Safety & Quality

Hello. This is Ellen Flink. I'm sitting in for Rachel Block this afternoon.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Great. Thank you, Ellen. Much appreciated.

Ellen Flink – NYS DOH OHITT – Director Research, Patient Safety & Quality

Thank you.

Deven McGraw - Center for Democracy & Technology – Director

All right. Terrific. I'm glad that we got that taken care of, so we can jump right in. Today is actually our last scheduled call before the next Health IT Policy Committee meeting, which is, I believe, on the 19th of May. And so after our last calls where I think – I don't know about the rest of you, but it was certainly a bit of a frustrating call for me, and it wasn't anyone's fault, but I think that we presented with the task of thinking about how consent, which is really one element in a comprehensive framework of privacy protections, was needed or not needed based on different models was a difficult one for us to get our arms wrapped around because we didn't know enough about the models. We were sort of focusing on models as though they were definitive when one could have easily foreseen that there might be a kind of mix of models and maybe those models would apply in a snapshot in time today based on work that the NHIN Direct folks are doing, but it didn't necessarily mean that those would be the models going forward.

Without any really clear information about issues like how much data was going to be accessed, used, and disclosed, either in the message header or in the content or payload and what that information was necessarily going to be used for, I think we were having a high degree of difficulty in saying to what extent should consent, this sort of one piece of a bigger puzzle would apply. And I might almost characterize it as us being very reluctant to say that we necessarily didn't want consent given how little we knew about these models, how they would work, how representative they necessarily were of what was going on out there today, much less in the future. And without that set of questions, we certainly were not willing to necessarily take consent off the table except there was some degree of comfort with a model that didn't use an intermediary at all.

In a second, I'll get to what I think I'm proposing as our definition for an intermediary. But even in that context, some of us expressed suspicion about whether there would be a large number of transactions that would take place where an intermediary wasn't involved, and without sort of knowing the rules of the road for intermediary use of data, both in terms of the privacy aspects, as well as security, I just got a sense that we were not terribly comfortable with weighing in on patient consent. And I think, in hindsight, that makes sense.

What I did was to create a set of recommendations that I thought kind of refocus us a little bit and put consent in a broader context of a framework of protections and sets of policies that are both about policies on information, as well as some sense of what the technical requirements would have to be to support those policies, and to sort of do the hard work of setting those up, upfront, of which of course consent would be a piece of that, but does not become the lynchpin of the conversation. Otherwise I think we're inclined not to be terribly happy about saying you don't need consent in certain circumstances because we don't know if there are sufficient protections that would apply across the board.

What I did here, and there's a lot of text. You know I'm a lawyer, and I like to write, and this may be more than what we might put in front of the policy committee in terms of what is digestible in a short period of time, and we can talk towards the end of the call when we're able to have a more full discussion of the recommendations in here about what's the most effective way to get this across. But to me, the framing of it is very important, especially since we really sort of started out this exercise looking at what is the role of consent. And what I've put in front of you for consideration today is a variation on that, which is to very clearly say it's not just about consent. Consent is a piece of this, but we really need to get to the work of establishing, of taking essentially the set of principles that ONC adopted a couple of years ago and getting far more specific about the policies that would govern exchange at a variety of levels with NHIN Direct as really just the start.

Joy Pritts – ONC – Chief Privacy Officer

Deven, this is Joy, and I'd like to interject here.

Deven McGraw - Center for Democracy & Technology – Director

Sure.

Joy Pritts – ONC – Chief Privacy Officer

Which is that I agree that NHIN Direct should not be the focus of this, and I thought that in our last conversation, the workgroup's last conversation that a broader approach of trying to examine what factors began to cause people a discomfort with sharing information were beginning to be identified, like where is the pressure point. And I've read the screening, and I appreciate the work that has gone into it, and I believe that this workgroup was beginning to drill down on some of the factors of the higher privacy and security framework that ONC had put out in the past. But I guess where I am on this issue right now is we have programs here that are going to be getting, beginning to share data in 2011.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Joy Pritts – ONC – Chief Privacy Officer

This group meets once a month, and so we already do have some recommendations from past experience from NCVHS, and we're really hoping to get some recommendations from this group on some concrete issues. But these programs are going forward, and they will go forward with this group's great recommendations or without if the group isn't able to make any recommendations. So we are hoping that some recommendations can come out of this, but it is not going to – we cannot wait a year for an entire set of issues to be vetted and put together in a package and presented to us. It just isn't going to work that way because we don't have that; we don't have a year now.

Paul Eggerman – eScription – CEO

Joy, this is Paul Eggerman. Yes, I hear what you're saying. I'm wondering. Would it be possible to give us a schedule or something that says these are the specific areas that you need recommendations on, and these are the dates?

Deven McGraw - Center for Democracy & Technology – Director

Well, although, I'm going to push back on that, Paul. This is Deven. Joy, I understand that we're working on a timeframe that doesn't work very well for our current policy committee, much less workgroup schedule, and that's a challenge, but number one, I do think we have some recommendations in here, number one. Number two, again, if what's being presented to us is, okay, what's your policy on consent, I guess one answer would be it would be inadvisable to opine on that without having a set of very clear rules and an environment in which we understand what we're asking patients to consent into or giving them the rights to consent out of. Otherwise I'm almost inclined to say, yes, we should just have consent for everything because we don't have any rules.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Deven, this is Kathleen. No, I agree with you, but I also think we basically kind of touched on what this group's feelings are in this area and that we could actually use what you've written, but also just articulate what we've talked about before. And come up with some pretty simple, clear principles that would help guide our statements about where consent might play and where other kinds of controls and regulations might play. And I think the patient ... elaborate, a brilliant place to start.

Joy Pritts – ONC – Chief Privacy Officer

Kathleen, I'm going to have to interrupt you just one second here. Would whoever is typing real close to the phone please move your....

Deven McGraw - Center for Democracy & Technology – Director

Yes. No, actually, please mute your line. Thank you.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Is it okay if I just talk about this a bit?

Deven McGraw - Center for Democracy & Technology – Director

Sure.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Okay. I think that health information exchange should meet patient expectations about how their health information is shared, except for where the exchange is already governed by other laws that we're not going to be considering right here. For example, the exchange of sensitive information according to CFR, state laws in that area, research and public health. I think patients and I think the workgroup has said this that patients do not expect to make choices about their health information being exchanged in the manner intended by their providers to accomplish care delivery. I think patients do expect choice about their health information being exchanged in the manner not intended by their providers ... were not intended by their providers in the course of accomplishing care delivery. I think that just taking that toggle, you could look at it and say that the workgroup seems to be okay with direct exchange from the patient's providers to other covered entities where there's no intermediary in the middle that can access....

Deven McGraw - Center for Democracy & Technology – Director

Right.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

But if there is an intermediary that can access PHIs for routing and some very limited value added services such as translation and provide a directory, which would facilitate the intent of the provider who is sending the data, then there should be enforceable oversight to insure that any intermediary handling the data is doing so only on behalf of the sending covered entity. And where it goes beyond that, there should be some very clearly articulated rules about what – and I think you've laid it out here: constraint on access, collection access, use and disclosure, and constraints on data retention and reuse, which might be something that ONC could – and other ones you have here – that ONC could maybe articulate in guidance or regulation or HHS could.

But where an exchange system cannot verify that the provider or covered entity requesting health information has a treatment relationship with the patient whose records are being queried, then the exchange system must allow the patient choice about whether their health information is available and accessible. I think we could take those three pieces and sort of come up with some recommendations that might be actionable by HHS. Does that make sense to you?

Deven McGraw - Center for Democracy & Technology – Director

Yes, it does, although, so here's what I would say. I think we essentially do have that recommendation in the stack, which is to say if you're in a set of circumstances where there's no intermediary involved, and I offer a definition because that got raised on our previous call of what constitutes an intermediary and what's not an intermediary, and I suggest that the term intermediary refers to an entity in the middle that has access to some data at any layer of the stack. So that would be at the content layer or the message layer in order to perform a function that facilitates exchange or provides some sort of value added service. We do say that where there's no intermediary involved by that definition, we have some level of comfort.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

But I think we need to go a little bit further because, for the most part, exchange always involves an intermediary.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

One or more intermediaries, and I think the dividing line that would meet what I think the intention was that the intermediary should have no access to PHI.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

And put the line there, and then say in between that and systems that allow entities to query data where they may not have a relationship with the patient, there is some gradation, and the one that's closest to that line of no access to PHI if some minimal access to PHI related to routing and addressing. And then there's the more complex value added pieces that start getting you into this area where there probably need to be some constraints in business associate agreements and other mechanisms, maybe consent at that level. And then the third place is basically what people think about as a RHIO or an exchange environment where entities can actually query for data where they may or may not have a treatment relationship with the patient, and that the provider who initially sent the data didn't intend it to be available for those purposes.

Now that said, there are RHIOs where a provider can be sending data to the RHIO for the purposes of getting it to a referring provider that they intended to get it to, and that provider can – it can be established that that provider has a treatment relationship, maybe even in the – I don't know what the mechanism is, but I think that's the line dividing when consumer/patient choice should come into play.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Judy Faulkner – Epic Systems – Founder

That was Rachel, right? This is Judy.

Deven McGraw - Center for Democracy & Technology – Director

No, that's Kathleen Connor.

Judy Faulkner – Epic Systems – Founder

Kathleen, I'm sorry. Kathleen, you said every exchange has an intermediary. Could you define what you mean by that because if in fact one healthcare organization sent something to another healthcare organization, and there is no one else other than that healthcare organization who can access that, is there really an intermediary there?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Well I guess that would depend on how you define intermediary. If you have a portal scenario, may that falls out, and I'm not ... trying to set some general parameters where even sending e-mail, you've got ... in the Internet that are going to be looking at the IP and could actually detect all sorts of information based on what's flowing through those nodes. And that's a deeper issue that I don't think we should go into here, but it's more at the principle level. If there is an intermediary that is moving things along and can do other than intended, that's the issue.

M

I think I agree with the concept, Kathleen. This is.... The thing I wanted to clarify is that there some exchanges that don't actually involve any intermediary. What we do at our sites is actually there is no intermediary other than, you know, the wire, the Internet basically, and I know there are switches and such in the Internet, so it depends on how deep you'd like to drill to find an intermediary, but there is no other weigh station of the data that really flows....

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Yes, and if you'll....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is Dixie Baker. I think that we do need to clearly define intermediary. I mean, we're tossing that term around ridiculously in my mind. I mean, if one enterprise sends information to another, and the data are completely encrypted, and it just goes through nodes on the way, there's no intermediary. I think that we need to clearly define what we mean by intermediary.

The other example I would bring up is we may have – it's quite common for covered entities to have business associates that perform services in their own, in the covered entity's facility. If that business associate performs some, I don't know, repackaging or translation into, let's say they translate it into the required codes, is that an intermediary? I think we need to clearly define that term and not just throw it around so cavalierly.

Deven McGraw - Center for Democracy & Technology – Director

Well, but this is – I need to grab. I want to try to focus this discussion a little bit, and to use it actually to hammer home a point, which is that all of the conclusions that we're able to draw are, in many ways – let me rephrase this. We're making a lot of – this just underscores the need to drill down at a more intense level if we think it's possible to do so as a workgroup. Otherwise, we're just going to have to make general recommendations that staff would have to continue to flush out.

But there are so many policy assumptions that are imbedded into this line of conversation that we have had over the past three to five minutes that, to me, underscores that you need some very clear rules, some very defined terms. Sort of assuming the data is encrypted, and so, therefore, there's no access to it. Well, we can't make that assumption, but we surely could make that a policy requirement if we could get to that level. The issue of sort of both....

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

...get to that level?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Joy Pritts – ONC – Chief Privacy Officer

Why don't we take one of these and try to get to that level?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I agree.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

I had the first one. This is Kathleen. The first one I named was no access to the PHI, so that would – encryption would have solved, would have fallen in that bucket.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Exactly. Let me first. I want to make sure, because we tend to have these conversations dominated by the few of us that have really strong opinions on this. I want to gauge people's comfort level with the sort of top line recommendations that I did put forth here, and I'm perfectly happy with trying to drill down on them and get more specific. But at this very top line, this recognition that while we started with this lens of consent, we need to make very clear that it is not the beginning, not necessarily the beginning or the end of the conversation.

That it plays a role and that data protection is very model dependent, and we need to be thinking about issues like what data can be collected, accessed, used, or disposed by an intermediary. What qualifies as an intermediary? What are the sort of embedded policy assumptions that shouldn't just be assumptions, but should be clearly stated and enforced through some mechanism of which consent is one of them, and then we can get to this, you know, start to really drill down on this.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Deven, this is Kathleen. I didn't hear anybody saying that consent is the end all, be all, so I think we pretty much agreed that it has a place to play in a larger framework.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I'm not. I wasn't suggesting. I mean, I just want to make sure that I'm getting full workgroup buy in on this.

Dave Wanser – NDIIC – Executive Director

This is Dave, and the thing I really like about what Kathleen laid out is you can understand it. Irrespective of that attorneys on the phone, there's a distinction between defining the policy and defining the definitions that are embedded in that policy.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Dave Wanser – NDIIC – Executive Director

And we tend to get, you know, the definitional piece of it is where we get mired down. A clear statement of policy that anyone could understand certainly is in the best interest of everyone. And then the detail falls out of the definitions for things like intermediary and consent.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Dave Wanser – NDIIC – Executive Director

But I really like the elegance of what Kathleen laid about because it clearly makes sense to people.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Dave Wanser – NDIIC – Executive Director

And you can explain it to a legislator or a physician or anybody else, and they go, oh, okay, that's what that means.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Gayle Harrell – Florida – Former State Legislator

This is Gayle Harrell as a legislator. I tend to be more of the nitty-gritty kind of person who really wants definitions and words have very significant impact later on, as things get, and in legislation, commas mean a whole lot, as things get interpreted. So I look for a little more detail, and I would love to see that in writing.

And also, I think we've got to come down to this definition of intermediary, and then you need to really – I like what Dixie said. You use things like encrypted. You know, nowhere in what you've laid out here, Deven, which I think is an absolute great beginning, but nowhere do we talk about encryption.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Isn't there a difference? Can we say something very high level about intermediaries and then describe what activities they're doing as the differentiator rather than, because, intermediary, we have to talk about the things in the middle, and we have to have a term for them, and what is different is what they're allowed to do with the data.

Joy Pritts – ONC – Chief Privacy Officer

But why can't we start out with articulating the principles and then identifying those words that need to be defined?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

I'm fine with that.

Paul Egberman – eScription – CEO

This is Paul Egberman. I have a comment about intermediary and what is being discussed. It's interesting, Deven. You used the word "model" at one point when you were describing what is going on. I just reread Latanya Sweeney's testimony that she recently gave, and she used the word architecture.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Paul Egberman – eScription – CEO

And what I'm wondering is the reason that we're getting tripped over this issue of what is an intermediary is what we're really tripping ourselves up over is this concept of architecture. Fundamentally, NHIN Direct represents an architectural approach, and that within that architectural approach, the words intermediary might have a certain significance, but there are other architectural approaches where the PHI, for example, is stored in an HIE as a noun, and is shared by various users, in which case the understanding of who the intermediary is different. I think the concept of what you're suggesting, Deven, is correct. But as we talk about definitions that Gayle and other people seem to be suggesting, in my opinion, you need to find two or three or four high level architectures that we're going to deal with, which is also consistent with the concept of contextual consent. Contextual consent is really the same thing as depend on what the architecture is

Joy Pritts – ONC – Chief Privacy Officer

Paul, having said that, are there areas? I understand that the group feels that it is not – I'm not going to put words in anybody's mouth here, but are there areas where you believe that there are general architectural approaches that you understand well enough to be able to address those?

Deven McGraw - Center for Democracy & Technology – Director

No.

Joy Pritts – ONC – Chief Privacy Officer

I'm sorry, but I was asking that to Paul also.

Deven McGraw - Center for Democracy & Technology – Director

Okay.

Paul Eggerman – eScription – CEO

When you say address those, I don't know what you mean by address those.

Joy Pritts – ONC – Chief Privacy Officer

Well you said that there are, that in order to start looking at these issues, that you needed to look at general architectural approaches.

Paul Eggerman – eScription – CEO

That's right, and it depends on the level of detail you want to address it, in my view.

Joy Pritts – ONC – Chief Privacy Officer

Well I think we need to address it at a fairly high level so that it can, for example, to be very directed, we have states who have received a significant amount of funding, many of whom are using what I would or at least have proposed, I believe, in their at least preliminary plans to adopt what we would consider to be a kind of traditional RHIO model. And some are federated, and some are more—

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Centralized?

Joy Pritts – ONC – Chief Privacy Officer

Centralized. Thank you. That word was avoiding me for the moment. And so we do have at least, I mean, do you think that those are well enough developed architectural approaches to at least begin the discussion on that level?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

This is Kathleen. The problem with the architectural approach is that you can use the same architecture to do both direct exchange and to do the pull type of exchange where someone is querying for data that they may not, that the patient may not have intended to have available to them or the provider had not intended to have available. So there is an issue just taking that approach. It's not that it shouldn't be part of it, but just as a point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's part of the architecture though, Kathleen.

M

Well, but the architecture that was just spoken about is stage two. Federated or central, you're talking about stage two.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

But the problem is that they're doing it now.

Deven McGraw - Center for Democracy & Technology – Director

They're doing it now.

Paul Eggerman – eScription – CEO

...problem, and I got the sense. Maybe I'm looking at it wrong. I got the sense that that's partly what's motivating Joy. It's like the train has left the station on a lot of these....

Deven McGraw - Center for Democracy & Technology – Director

It's leaving. That's for sure.

Paul Eggerman – eScription – CEO

And so it seems to me, I mean, maybe I'm looking at this too crudely. There are three models. There's a real direct connect that Judy from Epic just talked about. There's this sort of federated model, and there's the centralized model. And I don't know if that makes progress by talking about it in those terms.

Jodi Daniel – ONC – Director Office of Policy & Research

Yes. This is Jodi Daniel. I'm wondering. Somebody made the comment that you can use different architectures for different kinds of things. Maybe if you overlay, you can limit what we're talking about by the type of service, so is this really a direct exchange or is it really a query. Maybe different issues come up there, but if we say, well, we're talking about a federated model that doesn't include query, can we specify what we're talking about, both based on architecture and services to actually get some progress, and then see how that might play out if you talked about a different service with that architecture and take it that way?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

This is Kathleen. That works for everything but the direct, so you can have value added service and nodes that do both the query and do direct, so you could overlay the architecture with the different exchange patterns.

Deven McGraw - Center for Democracy & Technology – Director

Yes. This is Deven again. So I do think that the models matter, and we've sketched out potentially some broad areas of models, but of course, the devil is in the details. I mean, one, you know, you sort of have the traditional RHIO federated model, right? But even if you look in the consent paper that explores some of the different ways that states are already up and running or at least further along in the planning stages, they've taken that model and put some different bells and whistles on it, some of which make it look a little bit more like direct exchange versus query response. I mean, as always, these things are rapidly morphing, and I do want this workgroup to be able to provide some more clear guidance.

But I think, number one, for us to really do that effectively would probably require us to meet more often and do a lot more background work in the interim, which I'm not opposed to, but I do think that we want a body of policies that are responsive to the various models out there and that absolutely deal with the issue of patient consent, but that it's important, but appropriately reflect the fact that we've got – you know, that that comes as a constellation of ideally of other policies about, that sort of more specifically apply that framework to these specific sets of circumstances and models. Maybe that's too much detail work for our workgroup, but I just feel like that's where we ought to be heading. And whether we, as a workgroup, continue to do this at a sort of broader level and feed into this process or whether there's a better way to do it, I don't know.

But we just have continually had so many questions about the details about how this functions. I mean, we got those lists of models just for NHIN Direct, and we had lots of questions about the sort of assumptions that were embedded within them, and ideally you'd want to crack that open in a more detailed way, and in order to come up with a set of policies that places consent within that spectrum.

Joy Pritts – ONC – Chief Privacy Officer

Well I think that what we need to do, what would be useful for us is to have some recommendations at a fairly high level because we can't possibly address every iteration of a federated or centralized system. That is not going to work for us, and it won't work for them. They don't want us to address those things. We can't possibly. There's not enough time in the day or the world to do that.

What we have been asked to do by the state basically is they're getting ready to start designing their systems. They don't want to make, and they're getting ready. Paul, you had asked me about the timetable. I don't know all of the timetable here, but the reason that this issue, the consent issue and the data segmentation issue were first teed up is because this fall is when the states have to begin. They have to submit their formal plans, and it's my understanding that they're going to begin to sign their contracts with their vendors shortly after that.

They have expressed to ONC in no uncertain terms that they're not going to be very happy if after they have signed contracts with their vendors that ONC were to come up with a policy that said, oh, and by the way, you better really make sure that you have some sort of patient choice in your model because that could be very expensive. So what we're asking, trying to ask is some fairly general guidance for them. Some recommendations so that we can give some guidance to the states in specific, I mean, since we're talking about specifics.

Sure, general guidance about policies that can go across the board are very useful, and the privacy and security framework that ONC developed a couple years ago is at a fairly high level, as are most fair information practice models. But what we need is something a little bit one layer down or two layers down that says to give them enough guidance that at least initially when they're signing a contract, they'll know generally what they need to put in on at least a large scale level, and that has to happen fairly quickly. So does that help, Paul?

Paul Eggerman – eScription – CEO

Yes. It's also just an observation I have. In my experience, groups of people can do amazing things, and they know when they have a deliverable and they have a deadline and a date. In the absence of that, we can spend two years defining intermediaries. I mean, because it's a really very interesting thing. We spend a lot of time on that one word. But also, the way I look at it is we exist for one function is to help the ONC staff.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Paul Eggerman – eScription – CEO

So that's the only reason we exist. If the ONC staff, if we're not helping them, there's no reason to have a discussion, have a call. And if they need something, we need them to tell us what it is they need, and specifically, again, what do you need, and when do you need it by? And then we'll do our best to get you that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is Dixie. It seems to me like if we really stand back and reduce this to what we truly care about, what we truly care about are information, and I'm not saying data, information, in other words, data that has meaning, so PHI, PHI visibility and PHI persistence. And it seems to me, if we came up with rules around who can actually see and manipulate PHI, unencrypted PHI, and who can persist it, keep it on their server, if we came up with rules about those two things, it wouldn't really matter what the architecture is and whether it's a push or a pull or intermediary or whatever if we just came up with rules on who can see the information and who can keep the information. We'd have a lot of this tackled.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

This is Kathleen. That's why the third suggestion I had was didn't even use the word intermediary. It was that if the system couldn't verify that the entity who was trying to get access to ... you're talking about, and....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Information.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Information, as you say, in the clear, and persistence being a second piece of it, access use and the actual collection, separating out those different things.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, I wouldn't even ... collection or use. I'd just say ... and keeping it, seeing it and keeping it.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Okay. But I said collection, access, use, and disclosure, but you can call it the way you want. That's fine. I think the piece that I believe we've been hitting on is that the requestor should be able to verify that they have a treatment relationship with the patient and that the sender intended them to have access, at least as a starting point. And if it's not verified, that the consumer choice or patient choice should be part of the picture.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But see, even there, that's a good example. Even the term access, I think you're really talking about whether you can see the information in the clear. If you can access the information, and it's encrypted, I don't care.

Deven McGraw - Center for Democracy & Technology – Director

Hold on. I don't want to get – I don't want to dive down this – this is a little too much detail. I want to try to get at what we're able to say today and almost a work plan for going forward. I want to get back to something, Joy, that you said about providing maybe one to two layers down of policy from the framework, which would include a consideration from consent, but which would allow us to get a bit more specific and where it's architecture or model dependent, we could go there. But probably not down necessarily into the ultimate level of detail because I'm not sure that we, as a workgroup, could necessarily do that in the timeframe. But is that what you're talking about, because that seems, to me, very appealing?

Joy Pritts – ONC – Chief Privacy Officer

Some of the key issues that we need to be – have resolved first, again, this goes back to what Paul had asked at the beginning of the call where the two that are on this group's agenda because I have experts on the phone, and you can correct me. But I understand that it's very expensive to retrofit those.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Joy Pritts – ONC – Chief Privacy Officer

The other point I would like to make, which is going a little bit to what Dixie was talking about, which is, I've heard a lot from some of the people on this call about revisiting very detailed requirements in HIPAA.

And maybe that is something that you would like to recommend at some point, but that is not going to help us in the short-term.

Deven McGraw - Center for Democracy & Technology – Director

Okay.

Joy Pritts – ONC – Chief Privacy Officer

Okay. So if the recommendation is these things need to be looked at, or there needs to be a general protection, some kind of things or HIPAA is fine the way it is. We don't need anything else. That's fine. But we don't have the time right now to delve into a lot of the specific elements of HIPAA.

Dave Wanser – NDIIC – Executive Director

This is Dave. The discussion about how many levels down in the detail we go, it seems like we're kind of starting with the lower levels of detail and working our way to the surface, and maybe if we started at the surface and worked, you know, got a clear statement of policy there, then separating what's definitional, what belongs, and what doesn't belong might be a little easier, but I don't know that we've gotten a clear statement of policy at the highest level yet.

Joy Pritts – ONC – Chief Privacy Officer

I think you're right, but the clear ... for consent for example, the clear state of policy right now, at least with respect, I'm going to break this out into a particular function just to focus the discussion on one little item that we could potentially look at. Let's look at treatment because that's one of the purposes that they're talking about sharing. Everybody is talking about sharing this information for.

The policy right now in the HIPAA privacy rule is that for most clinical information, information can flow for treatment purposes without the individual consent. And so what the states have been asking us has essentially been, are you going to – do we need to do something else? Do we need to ask, because of this new way we're holding health information, or is that still okay?

Gayle Harrell – Florida – Former State Legislator

Joy, I think that addresses the issue that Latanya brought up. It depends between push or pull. If it's push, and doctor A has referred the patient to doctor B, and doctor A is pushing that information to doctor B, obviously not.

Joy Pritts – ONC – Chief Privacy Officer

No, I'm going to stop right here, Gayle, and go into a little bit of what you said, which is, first of all, I don't want to get into a long discussion about what the term push means on the phone because we all know what Gayle means is that the doctor A initiates this transfer of information to doctor B. Is that correct, Gayle?

Gayle Harrell – Florida – Former State Legislator

Correct.

Joy Pritts – ONC – Chief Privacy Officer

Doctor A has knows that doctor B has a relationship or will have a relationship with the patient.

Gayle Harrell – Florida – Former State Legislator

Correct.

Joy Pritts – ONC – Chief Privacy Officer

We have two factors that Gayle has proposed, I think. Her scenario is that when a provider, for example, wants to disclose information to another provider electronically at their own initiative for treatment purposes that no additional consent would be required under HIPAA. Is that accurate?

Gayle Harrell – Florida – Former State Legislator

As long as that is not going to – if that's a direct exchange. That goes back to the question we were talking about ... intermediary. You're going to ... exchange, I think that's already been established, and we're all in accord with that. When we get to the query stage—

Joy Pritts – ONC – Chief Privacy Officer

Wait. Is everybody in accord with that?

Judy Faulkner – Epic Systems – Founder

No, this is Judy. I think it's okay, but I think it has limitations. The situation may very well be that the patient shows up in the emergency department that the doctors in that emergency department, the doctors who are going to receive the information query the other healthcare organization, know individual physicians, knows about this ahead of time, but the healthcare organizations have approved that they will exchange in general with a group of others who are in this exchange. The healthcare individuals are not watching those queries one-by-one. They don't have a person sitting there. But the approval has been given in advance to join this group of exchange people who have agreed to abide by whatever rules, and the information automatically goes back. It isn't that each one knows.

Joy Pritts – ONC – Chief Privacy Officer

And so you're saying that, and when you say the approval has been given, do you mean that the individual has given the approval or that the providers have approved?

Judy Faulkner – Epic Systems – Founder

Well, it's several things. It's the organizations have approved, so St. Elsewhere has agreed with the state hospital, and others in that state, and even others in the region or in the U.S. that when their patients move back and forth, they will agree that they will share information on them.

Joy Pritts – ONC – Chief Privacy Officer

Judy, I think....

Dave Wanser – NDIIC – Executive Director

I think that's a different scenario than what was initially....

Deven McGraw - Center for Democracy & Technology – Director

Yes, I do too.

Judy Faulkner – Epic Systems – Founder

It is, and that's why I think we have to address that one because that's going to be a big one.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Joy Pritts – ONC – Chief Privacy Officer

Can we start with the first one?

Judy Faulkner – Epic Systems – Founder

Okay.

Deven McGraw - Center for Democracy & Technology – Director

So we're back to, I think, the conundrum that we got in. Many calls ago, we largely got comfortable with sort of what I would label unfacilitated – not unfacilitated, but with no intermediary. So hold off on this for a second that we don't have an intermediary in the definition per se, although I did try to create one to say that that picture, assuming that we have basic protections on how that data moves, like that there's identification and authentication and the trust framework pieces that the NHIN workgroup is working on and that data is encrypted in transport. There are some assumptions that we may be making that contribute to our comfort level.

But largely for the transactions under stage one of meaningful use, we were comfortable that, again, not without any policy, but with some minimal policies like the ones I discussed. I may not have named them all. That we wouldn't apply. We wouldn't think that additional consent could be required. When we started looking at....

Joy Pritts – ONC – Chief Privacy Officer

I would like to reach some closure on this one before we move on so that we could have a recommendation out of the workgroup. Can we have at least a vote on that one?

Gayle Harrell – Florida – Former State Legislator

And I think you need....

John Blair – Tacanica IPA – President & CEO

This is John Blair.

Deven McGraw - Center for Democracy & Technology – Director

Hold on. Let me let John go.

John Blair – Tacanica IPA – President & CEO

Yes. Just one thing: I'm fine with that one that we're having a vote on, but I would say that one does require an intermediary.

Joy Pritts – ONC – Chief Privacy Officer

And other people on the phone have said that they don't use an intermediary.

Deven McGraw - Center for Democracy & Technology – Director

Okay. So let me....

Joy Pritts – ONC – Chief Privacy Officer

Can we just limit it, please?

Gayle Harrell – Florida – Former State Legislator

And let's put ... let's verbalize those assumptions. Let's verbalize the authentication, the encryption.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Gayle Harrell – Florida – Former State Legislator

Verbalize....

Joy Pritts – ONC – Chief Privacy Officer

Do you want to assume or the time being that both entities are HIPAA covered entities and then you have the security rule apply?

Gayle Harrell – Florida – Former State Legislator

Absolutely.

Deven McGraw - Center for Democracy & Technology – Director

Right, although doesn't a security rule not specifically require folks to use encryption?

Gayle Harrell – Florida – Former State Legislator

No, it does not.

Joy Pritts – ONC – Chief Privacy Officer

It does not, but it does have other functions in it. It is what the law is right now.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Gayle Harrell – Florida – Former State Legislator

But are we assuming encryption, authentication of the receiving person and encryption of the data?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

I'd like to assume that they're at least covering....

Gayle Harrell – Florida – Former State Legislator

And covered entity.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

...of safe harbor for breach notification so that, in transit, it's encrypted.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I think we can't use the covered entity to covered entity. I mean, if we wanted to approach stage one, because we've got transport to public health authorities and to payers for authentication checks, so that would be....

W

The payer is a covered entity. The only one....

Deven McGraw - Center for Democracy & Technology – Director

Right, the public health authorities.

Joy Pritts – ONC – Chief Privacy Officer

Again, what we're trying to do, first of all, I thought, was to find one area where the group might be able to agree before we moved on to different, what I want to call, use cases that you're examining.

Dave Wanser – NDIIC – Executive Director

And I think we're fine with that. But again, I'm going to come back to it. I don't think that there's a situation where you don't use some type of intermediary for what you've described.

Joy Pritts – ONC – Chief Privacy Officer

And I would agree that it should be, we can group the portal scenario and intermediaries who have no PHI access and them together.

Gayle Harrell – Florida – Former State Legislator

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I did try to define intermediary as having access to information, so maybe I shouldn't say data, Dixie, but to information either in the message or in the content.

Dave Wanser – NDIIC – Executive Director

So are you saying that they can persist it and view it, as Dixie described?

Deven McGraw - Center for Democracy & Technology – Director

No. I'm saying I'm assuming that they can't. I'm assuming, yes they can. Otherwise they're not an intermediary.

Dave Wanser – NDIIC – Executive Director

That's why I think it's the definition we need to talk about because I think the intermediary can be not doing either of those two and still be an intermediary and transporting it.

Deven McGraw - Center for Democracy & Technology – Director

Right, but I'm talking about defining the intermediaries that concern us versus the ones that don't.

Dave Wanser – NDIIC – Executive Director

We should at least call that out and say concerning intermediaries versus non-concerning.

Joy Pritts – ONC – Chief Privacy Officer

But can we talk about the data that they're looking at? It can either be data, or it could be PHI.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Information, please use the term information.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Yes, but there's a difference, Dixie, because....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

...talk about ... it means something....

Deven McGraw - Center for Democracy & Technology – Director

I know. I know. I know. Hold on. Hold on, let's....

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

...addresses and the file name of the content ... may not fall under, you know, information. It looks like data.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

If it's data, I don't care about it. If it has....

Deven McGraw - Center for Democracy & Technology – Director

Stop. Please stop. Let's take this conversation up to a level where somebody who is not steep in standards and technology can understand it. I think what we're concerned about is information.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Right? In particular, information that qualifies as PHI, or is that one level too far?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No, that's exactly what we're concerned about.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

That's what I was trying to say. Some information, and there's some data that might be used for routing that would not be concerning.

Gayle Harrell – Florida – Former State Legislator

We need to differentiate the definition of data versus information.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's established. I mean, that's well established. Data are bits. One is in zeros, and information has meaning. So that's what we really care about. If a bunch of encrypted bits flows through some place, and through an intermediary, and they can't derive personal information out of it, I don't care. But if those ones and zeros can really be interpreted as Dixie Baker's health information, that's what I care about.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Exactly.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's why it's important that we make that distinction. It really is.

Judy Faulkner – Epic Systems – Founder

But then we better define what it means because I think for most of the people reading it, they won't know that.

Gayle Harrell – Florida – Former State Legislator

The public does not understand that.

Deven McGraw - Center for Democracy & Technology – Director

Right. We need to say, I think what we need to say is that concerning intermediaries, intermediaries of concern, or our definition of intermediary for purposes of our discussion is one that has access to identifiable information. How about that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Judy Faulkner – Epic Systems – Founder

All right. Here's another way of phrasing this. And I'm trying to capture this conversation, but my shorthand is not that good.

Deven McGraw - Center for Democracy & Technology – Director

I know. I have a note taker. She is taking notes.

Judy Faulkner – Epic Systems – Founder

We have the provider holding the PHI initiates the transaction. They send the data to another provider for treatment of the patient. No one other than the initiating provider and receiving provider can see or retain the PHI.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. That's exactly right.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

The information or PHI because...?

Deven McGraw - Center for Democracy & Technology – Director

Yes. I think it's identifiable information because PHI has a particular definition.

Judy Faulkner – Epic Systems – Founder

Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I agree. Yes.

Paul Eggerman – eScription – CEO

Although that doesn't....

Gayle Harrell – Florida – Former State Legislator

Identifiable information.

Paul Eggerman – eScription – CEO

That doesn't quite do this, the environment that Judy talked about where there's a relationship between, say, a medical group and an emergency room.

Judy Faulkner – Epic Systems – Founder

Yes, and we will get to that one next.

Paul Eggerman – eScription – CEO

Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

We're going layer by layer, Paul.

Paul Eggerman – eScription – CEO

Okay.

Joyce DuBow – AARP Public Policy Institute – Associate Director

This is Joyce. Just to be clear, and so we're assuming that the receiving provider, for example, has full responsibility and accountability for whatever happens to that PHI.

Dave Wanser – NDIIC – Executive Director

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Gayle Harrell – Florida – Former State Legislator

Absolutely.

Joyce DuBow – AARP Public Policy Institute – Associate Director

Okay.

Deven McGraw - Center for Democracy & Technology – Director

And I do think it's important to put in a set of assumptions about issues like identity and authentication and the use of encryption.

Gayle Harrell – Florida – Former State Legislator

Absolutely.

Joy Pritts – ONC – Chief Privacy Officer

I think that's right because otherwise it could be loosey-goosy on the other end.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is Dixie. I'm not sure who just asked that question about the other end, but are we assuming that the entities at both ends are either covered entities or business associates, or can one of them be a PHR vendor, let's say?

Joy Pritts – ONC – Chief Privacy Officer

We're right now in this model, this little piece that we're looking at assuming that we're talking about, and this is Gayle's model, right, Gayle?

Gayle Harrell – Florida – Former State Legislator

Yes, my model. I don't know.

Joy Pritts – ONC – Chief Privacy Officer

We're talking about a providing sending information to another provider.

Dave Wanser – NDIIC – Executive Director

Right, for treatment purposes.

Gayle Harrell – Florida – Former State Legislator

For treatment purposes.

Dave Wanser – NDIIC – Executive Director

Right.

Joy Pritts – ONC – Chief Privacy Officer

Right, and I think that we are assuming that the privacy rule and the security rule are in place.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Gayle Harrell – Florida – Former State Legislator

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Yes, we are. But I'm not sure that it answers all of the questions that we would want to....

Joy Pritts – ONC – Chief Privacy Officer

It may not ... it is an assumption.

Deven McGraw - Center for Democracy & Technology – Director

Right. That's right.

Gayle Harrell – Florida – Former State Legislator

...also have to do your assumptions on encryption and authentication.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Right, because those are only addressable under HIPAA. So if we want to....

Joy Pritts – ONC – Chief Privacy Officer

So then that's the next piece. If that's really important to this group, does that involve consent, or does that involve...?

Gayle Harrell – Florida – Former State Legislator

No, this model does not involve consent.

Deven McGraw - Center for Democracy & Technology – Director

No.

Joy Pritts – ONC – Chief Privacy Officer

So why don't we put that in a parking lot?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

It doesn't involve consent, but I think patient expectation is that their data can't be ... over the wire, and that a breach would not be possible because it was encrypted.

Gayle Harrell – Florida – Former State Legislator

Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right. We said they were HIPAA compliant.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

But HIPAA doesn't require the encryption. That's all.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, it does. It requires that, I mean, privacy rule requires that you not expose PHI to people who aren't authorized, and so the security rule requires that you at least address encryption and encryption is the only way I know to....

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

...suggesting that it be required, not just addressable.

Deven McGraw - Center for Democracy & Technology – Director

Which is in fact, we made that recommendation already, and so we should go back to it and state it again.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

You don't lose by restating those kinds of things.

Deven McGraw - Center for Democracy & Technology – Director

No, definitely not.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

...talking when the public hears the recommendations.

Joy Pritts – ONC – Chief Privacy Officer

That's right, but I'm ... that's right, so let's put that as a separate recommendation, all right, because it deserves to be – since you pulled it out before, maybe you want to pull it out separately again. Do you want that separate?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

What is that recommendation? Would somebody...?

Joy Pritts – ONC – Chief Privacy Officer

The encryption element of the security rule should be required not addressable.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Absolutely.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

And that should be for all the exchange patterns, so maybe that is sort of something to put aside and look at....

Deven McGraw - Center for Democracy & Technology – Director

Yes. I mean, we had already stated. Keep in mind that not just for encryption, but for any of the security functionalities that were in the IFR, we already stated that we wanted to make sure those got used.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, that's the key is that even in the IFR, it requires for certification that you be able to encrypt using AES, right? But the policy is the part, and even if we made the HIPAA encryption required instead of addressable, we still need the policy piece to say PHI, identifiable information that's sent over an open or an open link, even if it's wireless, needs to be encrypted.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

...because it's not, we're not just going to be talking about covered entities who are also taking advantage of the meaningful use incentives.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But that's my point. Even a meaningful use incentive doesn't require that they use the encryption. It just implies that they have encryption.

Joy Pritts – ONC – Chief Privacy Officer

Right, so what you're saying is that you made your recommendations. I'm just trying to summarize what you said. What you said in the past was that meaningful use requirements should require encryption.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Joy Pritts – ONC – Chief Privacy Officer

And what you're saying now, I think, is an expansion of that, which is it should be in the security rule itself.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No, because the security rule, if anything, it should be in the privacy rule because the security rule just specifies the mechanisms that they have to support.

Deven McGraw - Center for Democracy & Technology – Director

I think it's much more of, I think we can say that there are a set of conditions that apply to our being comfortable with this sort of set of scenarios where we don't think additional patient consent would be needed. And those include the identification and authentication and encryption of that data. I mean, maybe there are some others, and that's the difficulty is that we're sort of thinking about what policies we might want to make sure are in place beyond what current security rule requires, so I wouldn't want to be missing anything.

But, one, we presume current law applies. Two, we assume that it's direct. Three, we assume there's not an intermediary in the middle who can access individual information as part of the transaction. And, three, we do assume that there's some basic security policies that are being followed. I think I might have repeated two.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Including encryption and authentication.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Judy Faulkner – Epic Systems – Founder

And you're also assuming that each side knows.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Gayle Harrell – Florida – Former State Legislator

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

And may I go back to Joyce, Joy's comment about the security because I take that back. She's right. The security rule does have some embedded policy in it.

Joy Pritts – ONC – Chief Privacy Officer

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Like authentication, so yes. I think that that does make sense to make encryption, yes, encryption over open links a requirement in the security rule.

Adam Green – Progressive Chain Campaign Committee – Cofounder

This is Adam. Just to clarify exactly what the security rule says, encryption, there's encryption for transmission. There's encryption for storage. Both of them are addressable, which means that you are required to do it if it is reasonable and appropriate. So it's not, you know, I don't want people to think addressable means—

Deven McGraw - Center for Democracy & Technology – Director

You don't have to do it. Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Adam Green – Progressive Chain Campaign Committee – Cofounder

And, you know....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's a good point. That's a real good point.

Joy Pritts – ONC – Chief Privacy Officer

And if you can't, if you decide that it's only an addressable criteria, you have to document why.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Right ... have to do ... implement an alternative.

Joyce DuBow – AARP Public Policy Institute – Associate Director

Who decides if you've made the right decision?

Joy Pritts – ONC – Chief Privacy Officer

If you are audited....

Adam Green – Progressive Chain Campaign Committee – Cofounder

OCR.

Joy Pritts – ONC – Chief Privacy Officer

...make that determination.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Joyce DuBow – AARP Public Policy Institute – Associate Director

Yes, I would prefer to see it required though.

Gayle Harrell – Florida – Former State Legislator

Me too. I go for required.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO

Yes, and this is Paul Tang. I also support that. I'm still incredulous to that because my recollection was that somebody was reading from the security rule was that when it goes over the open Internet, it absolutely has to be encrypted.

Joy Pritts – ONC – Chief Privacy Officer

No, it's addressable.

Adam Green – Progressive Chain Campaign Committee – Cofounder

No, there's breach....

Dave Wanser – NDIIC – Executive Director

Paul is right. It's only internally that it's addressable.

Joyce DuBow – AARP Public Policy Institute – Associate Director

So when HIPAA was written, they were anticipating value added networks where everything was closed. They weren't anticipating the Internet.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO

Actually, no, that's ... if I'm recalling correctly, there was, I think the phrase was open network or something like that that differentiated the point-to-point. All of a sudden, I lost the words for the dedicated line versus the open Internet. I'm almost positive the open was encrypted.

John Blair – Tacanic IPA – President & CEO

Paul is correct. I'd have to go find the site, but I'm almost positive.

Joy Pritts – ONC – Chief Privacy Officer

Is that in the guidance from CMS?

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO

No, that's ... law.

John Blair – Tacanic IPA – President & CEO

I think it's in the rule.

Deven McGraw - Center for Democracy & Technology – Director

Adam?

Adam Green – Progressive Chain Campaign Committee – Cofounder

There is no place in the rule where encryption is required. It is addressable. And with respect to whether the open Internet was imagined, I mean, HIPAA was built around administrative transactions that there was an assumption this was going to be going over potentially open line. There's reference to direct data entry over the Web, so I think that is pretty clear evidence that the Internet was envisioned here.

Joy Pritts – ONC – Chief Privacy Officer

There is CMS guidance on secure transmission, and that may be the source of what you're thinking of, Paul. When I say guidance, I mean there was a document, and it was pretty detailed.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO

Are you saying that it should be encrypted?

Joy Pritts – ONC – Chief Privacy Officer

I believe that's accurate. I think that's where you're getting that from.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO

I think John and I are still, I mean, I almost see the words.

Deven McGraw - Center for Democracy & Technology – Director

Yes, but I'm sorry. I don't want to get into a lengthy discussion of this. We have representative from OCR on the call who is telling us the encryption is not required.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right. I think we need to go ahead and make that part of our recommendation that encryption be required.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Yes. If there's anything you want to send me afterwards for me to reconsider that, I would be ... you to do so.

Jodi Daniel – ONC – Director Office of Policy & Research

This is Jodi. Can I just ask? Encryption should be required for--?

Deven McGraw - Center for Democracy & Technology – Director

In other words, we're basing, we're saying that it ought to be part. It's part of what makes us comfortable about the sort of one-to-one exchange without an overly intervening intermediary per our earlier discussion.

Joy Pritts – ONC – Chief Privacy Officer

You're talking about for transmission.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

But it's an intermediary, even if they're not having access to the individual...?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Deven McGraw - Center for Democracy & Technology – Director

I was trying to piggyback on what I thought we had already decided, which is that....

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

...other piece though, that intermediary may be persisting the data, as Dixie was talking about before. So we may want to think about encryption at rest.

Joy Pritts – ONC – Chief Privacy Officer

Let's break off one piece of this at a time, okay?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

The encryption part for transmission, the privacy and security standards workgroup came up with wording for that when we were first reviewing the meaningful use stuff that really addressed the, you know, was phrased in terms of the possibility that the information might be sent over an open transmission link. And that was to incorporate all of the various types of wireless, as well as wired communications. Deven, I can resend you that, how we ultimately phrased that if you'd like.

Deven McGraw - Center for Democracy & Technology – Director

Right. That would definitely be helpful. Here's another question for you, Joy. I get that the states want guidance, and we need to be feeding into what's going on with NHIN Direct too, so I understand that there are a lot of balls in the air, and I totally agree with Paul Eggerman that we want to be as helpful as possible. And I get that the states might be asking about consent, but given that we've really struggled and, I think, for valid reasons at thinking about consent in the absence of knowing all of these other assumptions and feeling comfortable about them, wouldn't we be better to give states some guidance along some of these other lines as well rather than giving off the impression that consent is, you know, the question that is...?

Joy Pritts – ONC – Chief Privacy Officer

What do you think you can accomplish in the time allotted?

Deven McGraw - Center for Democracy & Technology – Director

Right.

Joy Pritts – ONC – Chief Privacy Officer

They are signing contracts in August.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I assumed that it would be helpful for you all too because we want to give them guidance. You want to give them guidance. Is it just on consent that you want to give them guidance on?

Joy Pritts – ONC – Chief Privacy Officer

We are trying to break this down. I understand that the proposal for doing this was to break it down into manageable bites.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Joy Pritts – ONC – Chief Privacy Officer

And if you're saying that the manageable bites you have to take will not start with consent, they're somewhere else, then I suggest thinking about that to see whether those other elements can be addressed after they sign their contracts or if they need to be addressed before. And I don't know the answer to that because I'm not a technologist. We were trying to identify the big ticket items that they really needed some guidance on before they moved forward. These were the ones that they had floated to the top.

Deven McGraw - Center for Democracy & Technology – Director

Right. In other words, are there any other sort of issues that would be difficult to retrofit later if we made policy on them and then asked them to adopt it three months in.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Isn't it the opportunity for choice as to whether a patient wants their data put into a system where it could be accessed and used or persisted for reasons that are outside of this initial comfort zone? Maybe we could start there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think we should pass on the kind of litmus paper that Paul Tang gave us about patient expectations. I mean, that was wonderful advice, I think, if in any given situation if a patient found out that their information was being used or disclosed in this way, would they be surprised.

Joyce DuBow – AARP Public Policy Institute – Associate Director

Yes.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Which comes back to what I think I said earlier is that it's about transparency.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Adam Green – Progressive Chain Campaign Committee – Cofounder

It's about the understanding of the individual as to what's going to be done with that information and how, which was....

Gayle Harrell – Florida – Former State Legislator

We have one recommendation right now on the table that we haven't voted on, and assuming encryption and authentication using the privacy rule and HIPAA for that one-on-one to one direct exchange, physician-to-physician. Can we at least clear that one with the assumption to verbalize?

Adam Green – Progressive Chain Campaign Committee – Cofounder

In terms of expectation, I don't see how that's any different from what a patient expects when he presents himself....

Gayle Harrell – Florida – Former State Legislator

I agree with you.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I agree. Gayle, I think that's a nice articulation. Is there anybody that objects to that? Okay.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Could you repeat it? A little louder, we're having a little trouble hearing you.

Deven McGraw - Center for Democracy & Technology – Director

Okay. I thought I was the loudest person on the phone.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

No, it was him.

Deven McGraw - Center for Democracy & Technology – Director

It was Mike.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Deven, you are the loudest person on the phone.

Deven McGraw - Center for Democracy & Technology – Director

I knew that.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

I wasn't the one making the motion here or stating the motion. I think....

Deven McGraw - Center for Democracy & Technology – Director

Yes, I think it began with Gayle.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Gayle, could you restate your...?

Gayle Harrell – Florida – Former State Legislator

I think Joy had it pretty much down. It's basically direct exchange, physician to other entities for treatment, physician to hospital, physician-to-physician for a direct one-on-one exchange with the understanding that there is encryption, authentication of the receiving entity in place, and it's for the treatment of the patient.

John Blair – Tacanic IPA – President & CEO

What does it mean, "authentication at the receiving entity", though?

Gayle Harrell – Florida – Former State Legislator

You know that that person getting it is who they are.

Deven McGraw - Center for Democracy & Technology – Director

Right. There's got to be identity at both ends.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Right.

Deven McGraw - Center for Democracy & Technology – Director

The trust framework that NHIN talks about.

Gayle Harrell – Florida – Former State Legislator

You don't want to dial the wrong number and send it to Joe's sweatshop.

Adam Green – Progressive Chain Campaign Committee – Cofounder

This is Adam. By the way, authentication is required. It's ... addressable.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Gayle Harrell – Florida – Former State Legislator

Required, all required.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Joy Pritts – ONC – Chief Privacy Officer

That one is encompassed in the privacy and security rule, right?

Gayle Harrell – Florida – Former State Legislator

It doesn't really matter whether it's encompassed or not if we make it our recommendation.

Joy Pritts – ONC – Chief Privacy Officer

Right, but I thought with the encryption piece that you needed to make an additional recommendation on that, so I was just trying to....

Gayle Harrell – Florida – Former State Legislator

Yes, we want to make it an additional recommendation. We want to see that.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Joy Pritts – ONC – Chief Privacy Officer

So we have encryption, which you would like to make it required as opposed to addressable element.

Gayle Harrell – Florida – Former State Legislator

Correct.

Joy Pritts – ONC – Chief Privacy Officer

You have authentication as part of the existing privacy and security rules.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Gayle Harrell – Florida – Former State Legislator

But rearticulated for public consumption.

Joy Pritts – ONC – Chief Privacy Officer

Okay. That's right. We can do that. We can leave that. I just wanted to make sure that we don't have to do anything else on that.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Encryption when it's persisted by an intermediary.

Joy Pritts – ONC – Chief Privacy Officer

We're not going there, Kathleen, because we're assuming that nobody can. Right now, well, maybe we can add that one later, right?

Gayle Harrell – Florida – Former State Legislator

Yes.

Joy Pritts – ONC – Chief Privacy Officer

It's provider to other provider. Is that...?

Gayle Harrell – Florida – Former State Legislator

Provider.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Gayle Harrell – Florida – Former State Legislator

That would include if you're sending an order for a lab test. If you're sending information to a hospital, you're sending information to a doctor.

Joy Pritts – ONC – Chief Privacy Officer

Right. And it's for treatment, right?

Gayle Harrell – Florida – Former State Legislator

For treatment.

Joy Pritts – ONC – Chief Privacy Officer

Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

What was the authentication piece?

Joy Pritts – ONC – Chief Privacy Officer

It's in there, and that no one other than the initiating or receiving provider can see or retain the....

Gayle Harrell – Florida – Former State Legislator

Information.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I'd like to make it clear that both the entity and the person have to be authenticated.

John Blair – Tacanic IPA – President & CEO

But a lot of times you're not going to have a person on the other end. Entities may be exchanging things programmatically.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

What you say is that the entity must be authenticated just to make it clear that....

Gayle Harrell – Florida – Former State Legislator

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Sender and receiver.

Gayle Harrell – Florida – Former State Legislator

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Must be authenticated.

Gayle Harrell – Florida – Former State Legislator

Yes, but make sure that it's the entity.

Joyce DuBow – AARP Public Policy Institute – Associate Director

If it's for treatment, somebody is going to be using it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I know, and they'll be authenticated too, but you shouldn't be able to send, you know, Dr. Jones from Kaiser should not be able to send patient information to Dr. Smith at UCLA with just Dr. Smith and Dr. Jones authenticated. It should also be authenticating the entities.

John Blair – Tacanic IPA – President & CEO

Can I suggest that the authentication...?

Judy Faulkner – Epic Systems – Founder

Then we're getting into what I was saying earlier.

John Blair – Tacanic IPA – President & CEO

I suggest that the entities need to authenticate for transmission because there are a lot of programmatic transmissions that can occur.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Exactly.

John Blair – Tacanic IPA – President & CEO

But then it's the destination entity's responsibility that any of its users that might access the patient's record need to authenticate pursuant to the current HIPAA standards that are already in place.

Gayle Harrell – Florida – Former State Legislator

Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Exactly right.

John Blair – Tacanic IPA – President & CEO

So we don't really need to talk about user authentication at this point in time because it already should be assumed.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right, it's....

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

How will they know? How will the sender guarantee that the dietitian at the hospital isn't also authenticated to...?

John Blair – Tacanic IPA – President & CEO

That's the covered entity's responsibility already.

Dave Wanser – NDIIC – Executive Director

Right. It's the policy of the company.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, I agree. Yes.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Yes. This is Adam. The security rule requires that you implement procedures to verify that a person or entity seeking access to an electronic PHI is the one claimed, which means that you're going to require. You're going to have to have authentication that the requestor, in this case we've got a directed push, so that's – and I apologize for saying push....

Deven McGraw - Center for Democracy & Technology – Director

It just comes so easily.

Joy Pritts – ONC – Chief Privacy Officer

Authenticating the user doesn't say whether they are authorized to actually receive or access the data. That was my point, and just relying on the policy of the receiving entity may not be enough if we really want to insure that the sender gets ... receiver that was intended.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

The policy....

John Blair – Tacanic IPA – President & CEO

But you can't dig into that level of detail.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, I agree. Yes.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Yes. You can't, and you also cannot – you also should not say in a recommendation and dictate to the entity who they will or will not authorize to authenticate to the system. we can hope that they wouldn't allow, you know, the dietitian to authenticate for certain information, but it's not our call.

John Blair – Tacanic IPA – President & CEO

Actually, it goes further than that. Each one of these, in theory, if these are covered entities, had obligations under HIPAA to appropriately authenticate their users anyway.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right.

Gayle Harrell – Florida – Former State Legislator

Correct.

John Blair – Tacanic IPA – President & CEO

So you should have the ability to rely upon a covered entity's representation that it is complying with HIPAA or, I guess, that that should suffice in order to do that level of authentication.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

I was trying to get to Gayle's....

Joyce DuBow – AARP Public Policy Institute – Associate Director

Can she say that? Can we just clarify that that's our intention?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Gayle Harrell – Florida – Former State Legislator

Yes, I think that needs to be part and parcel of it that the presumption is there that the receiving entity has an authentication and authorization compliance model in place under HIPAA.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think that's sort of a rat hole. I think we should just say the assumption should be that each of the connecting entities are compliant with HIPAA.

John Blair – Tacanic IPA – President & CEO

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Then we just specify the entity-to-entity connection and entity-to-entity encryption.

John Blair – Tacanic IPA – President & CEO

Yes, I agree.

Joy Pritts – ONC – Chief Privacy Officer

Agreed.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Yes. Agreed.

Joy Pritts – ONC – Chief Privacy Officer

Are we in agreement?

Adam Green – Progressive Chain Campaign Committee – Cofounder

It sounds like it.

Deven McGraw - Center for Democracy & Technology – Director

It sounds like it.

Joy Pritts – ONC – Chief Privacy Officer

Okay. The recommendation deals with, is based on the following assumptions that there will be, first of all, to start this off before I go into this particular one, there will be a separate recommendation that encryption should be required, not addressable under the security rule. Then assuming that that would be the case or that encryption is required or is actually utilized, and that authentication, as it is currently voiced in the HIPAA rules, is in place, and that the sending and receiving entities are compliant with HIPAA. There's no additional patient consent needed for a provider to send protected health information to another provider for treatment purposes when no one other than the receiving or initiating provider can see or retain the identifiable information. Is that right?

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

I think we were using identifiable information instead of protected, but....

Joy Pritts – ONC – Chief Privacy Officer

Yes, I did say protected.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Good save.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Agreed.

Joy Pritts – ONC – Chief Privacy Officer

I said, or retain identifiable information. Is that right?

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Joy Pritts – ONC – Chief Privacy Officer

I hope you have a good note taker.

Deven McGraw - Center for Democracy & Technology – Director

I do, but we have the – I do. She's probably going to IM me any minute and go, ah.

Sarah Wattenberg – ONCHIT – Public Health Advisor

But we also have a transcript.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Thank you, Sarah. That's great.

Sarah Wattenberg – ONCHIT – Public Health Advisor

I believe. Remember, I'm new.

Joy Pritts – ONC – Chief Privacy Officer

All right. That's progress. Thank you.

Deven McGraw - Center for Democracy & Technology – Director

Yes. That is progress.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I hate to say this. I have one more that we absolutely have to put in there is that the information is not only encrypted, but integrity protected.

Deven McGraw - Center for Democracy & Technology – Director

So that it can't be messed with along the line?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Exactly.

Gayle Harrell – Florida – Former State Legislator

Yes, it's important.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

...requirement, but just to place it....

John Blair – Tacanic IPA – President & CEO

By the way, if something is encrypted, the ability to modify it would be impossible or else your encryption would fail. So your integrity issue, this idea of integrity is assumed when you encrypt.

Deven McGraw - Center for Democracy & Technology – Director

Yes, I would hope so. Otherwise, what's the purpose of encryption? That's a good point.

John Blair – Tacanic IPA – President & CEO

Exactly, and so you really don't need to talk about integrity because it can't not be – if the encryption fails.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, you're right.

Adam Green – Progressive Chain Campaign Committee – Cofounder

It ... in the term.

Joy Pritts – ONC – Chief Privacy Officer

Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

And the protocols usually do both as well.

Joy Pritts – ONC – Chief Privacy Officer

Okay.

Deven McGraw - Center for Democracy & Technology – Director

And I think we can talk about the reason why we get comfortable with this. Again, it's not as though we don't foresee the need for some policies around it, but we're largely comfortable with not requiring additional consent because we've made some assumptions that certain things will be in place, and it's consistent with patient expectations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Should we mention that the accounting for the disclosure needs to be there?

Joy Pritts – ONC – Chief Privacy Officer

No.

Deven McGraw - Center for Democracy & Technology – Director

Let's take that up later, please.

Joy Pritts – ONC – Chief Privacy Officer

No, let's try to stick with a basic, you know, at this level, if it's okay, if we can reach agreement on this, because once you start down that discussion on accounting for disclosures, it's going to be a very lengthy conversation, and I would like to get a recommendation.

Deven McGraw - Center for Democracy & Technology – Director

I think you got one, Joy. I wish we could proceed to the next one. We will definitely, for folks who don't know, by the way, the Office of Civil Rights has a request for information out on the accounting of disclosure provisions in ARRA. It has a very tight timeframe. We could not, as a workgroup, bring things to the policy committee in time to respond to it, and there will be a subsequent rulemaking. But for folks who are interested, that is out and open for comment now.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Yes, you have until May 18th, plenty of time.

Deven McGraw - Center for Democracy & Technology – Director

There's your public service announcement, Adam. Yes, I think we can't. You know, that's not a provision that is yet in effect in law, and I think there are some issues that need to be worked out there, so I'd prefer to parking lot that one if we could.

Joy Pritts – ONC – Chief Privacy Officer

Now I would like. This is our recommendation, your recommendation, and I would like to go back just one step and see to clarify that if one of these elements was missing, then you would recommend that your recommendation would be that you would need to obtain the patient's consent?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

John Blair – Tacanic IPA – President & CEO

Yes.

Deven McGraw - Center for Democracy & Technology – Director

I think that's right, you know, and it's crazy because if you think about it, it's exactly the wrong position you want to put patients in, right? Like having them consent to a situation that you suspect is risky from a privacy and security standpoint because it doesn't have clear rules around it. But in the absence of those, we're not comfortable saying that it's okay not to give patients some rights not to be part of it. Is that a fair articulation?

Gayle Harrell – Florida – Former State Legislator

Yes.

John Blair – Tacanic IPA – President & CEO

Unfortunately, yes.

Deven McGraw - Center for Democracy & Technology – Director

It's terrible. You know, we end up positioning this as sort of, you know, we're looking at getting comfortable with a set of circumstances under which implied consent, essentially, is okay. Otherwise, we want to give patients some choice, even though we acknowledge that in doing so, we're giving them choice to a potentially bad set of circumstances, which is far from ideal.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Right.

Joy Pritts – ONC – Chief Privacy Officer

However, it's not out of line with what the GW paper recommended at the very end, if I remember right.

Deven McGraw - Center for Democracy & Technology – Director

Yes. No, which is interesting.

Gayle Harrell – Florida – Former State Legislator

I think, when you're putting patients at risk, they need to know it, and they need to, when you put their information at risk, they need to have input into that in the form of consent.

Joyce DuBow – AARP Public Policy Institute – Associate Director

But does that mean you actually have to sort of indicate when you're giving them the choice what the kind of risk is that they may be agreeing to?

Gayle Harrell – Florida – Former State Legislator

I think....

Deven McGraw - Center for Democracy & Technology – Director

Absolutely.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Yes.

Gayle Harrell – Florida – Former State Legislator

...to do that.

Deven McGraw - Center for Democracy & Technology – Director

But more importantly, I think it does argue for us to, you know, if in fact we don't want to put this all on patients, which we really don't.

Gayle Harrell – Florida – Former State Legislator

No, we don't. And we need to have a framework that eliminates as much risk as possible.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Joyce DuBow – AARP Public Policy Institute – Associate Director

Right.

Gayle Harrell – Florida – Former State Legislator

But patients need to know what's going on, and I think part of what ONC needs to do, and we need to make sure happens is that there's patient education in the entire endeavor.

W

But, you know, this just puts the patient in the classic position of being between a rock and a hard place because they're really not in a position to say no, you can't use my information. That just means the information won't be transmitted, which is probably not in her best interest anyway.

Gayle Harrell – Florida – Former State Legislator

But you still need to have – she needs to make that decision.

Deven McGraw - Center for Democracy & Technology – Director

Yes, but that's the very reason why I think we ideally don't want to put it on consent.

Gayle Harrell – Florida – Former State Legislator

Safeguards should not just be consent.

W

It's no different from the situation that we have today where you sign anything because you know you have no choice.

Deven McGraw - Center for Democracy & Technology – Director

Right. That raises another interesting question that I'm not sure whether it would lead to a recommendation or not, but I'm curious how the workgroup feels. Are there a set of circumstances under which even if we do in fact put a lot of safeguards, succeed in putting a lot of safeguards in place. For example, yes, there are intermediaries in the middle who have some access to identifiable information, but we have really clear rules that constrain their ability to collect it and persist it and use it and disclose it and reuse it. And where we very carefully limit the purposes for which exchange can be used to treatment and lawfully enacted public health requirements and some other pieces. Again, this is a hypothetical, so it's not fully flushed out. But are there circumstances under which even with a full set of safeguards, we would give patients a role in consenting anyway?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

This is Kathleen. I think there's more than risk at stake here, and controlling access. I think patients have a right to say I don't want that person to have access to that information. I think the example that the use case that Charles Kennedy brought up at a recent meeting where a patient's mental health medications were maybe revealed to a provider who might not have needed those reports ... whether they might have needed it in the course of care, those kinds of situations where it's a use that a patient did not expect or intend, and that's different than risk.

John Blair – Tacanic IPA – President & CEO

Deven, all the time patients decide not to give a provider certain information, so now this is giving an entity, an intermediary information. I think they should have that opportunity.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think that's why the Paul Tang rule comes into play because there are. I mean, I certainly know in my own experience, there are really creative people out there with things that are within the law, but if you really come back and say, what would a patient think, you'd say they need consent.

M

Yes.

Joyce DuBow – AARP Public Policy Institute – Associate Director

Yes. You're right.

John Blair – Tacanic IPA – President & CEO

Deven, this is John. I've got a question.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

John Blair – Tacanic IPA – President & CEO

Since we're not going to call this entity an intermediary, what do you call the entity that now for what we've agreed on doesn't require consent, but is taking the responsibility of getting that information from the provider to the other provider securely with authentication, etc. to the digital endpoint? What do you call that? If it's not an intermediary, what are we going to call it?

Gayle Harrell – Florida – Former State Legislator

How about transit agent?

John Blair – Tacanic IPA – President & CEO

That's fine.

Deven McGraw - Center for Democracy & Technology – Director

Transit agent? I like that term actually better than the one that they're using in the NHIN Direct conversations, which is HISP.

John Blair – Tacanic IPA – President & CEO

Yes, but you know they're going to end up calling that an intermediary.

Gayle Harrell – Florida – Former State Legislator

Yes. I like transit agent.

Deven McGraw - Center for Democracy & Technology – Director

Transit agent.

John Blair – Tacanic IPA – President & CEO

Bus driver.

Deven McGraw - Center for Democracy & Technology – Director

Bus driver?

Gayle Harrell – Florida – Former State Legislator

I mean, what are you doing? Is that not what you're doing?

John Blair – Tacanic IPA – President & CEO

Digital postal service, whatever it is, just so we have, so we can at least characterize it.

Deven McGraw - Center for Democracy & Technology – Director

Yes. That's a good idea.

Gayle Harrell – Florida – Former State Legislator

...courier, the idea of courier in the law already, doesn't it?

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO

How about conduit? Conduits don't have people in them.

Gayle Harrell – Florida – Former State Legislator

That's a good word.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Yes. That word actually even appears in HIPAA guidance right now as you're not a business associate if you're a conduit.

Deven McGraw - Center for Democracy & Technology – Director

Okay.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO

We don't want crying eyes there.

Gayle Harrell – Florida – Former State Legislator

Yes, that's good.

John Blair – Tacanic IPA – President & CEO

Although you may want business associate rules plus on the conduit, but again, as long as we have some term for it.

Gayle Harrell – Florida – Former State Legislator

Conduit works.

M

Yes, I like that.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

We use conduit, and are thinking that your going to have business associate rules apply to them, then you might have a problem because the HIPAA rules actually say if they're a conduit, they don't have to.

Deven McGraw - Center for Democracy & Technology – Director

Right.

John Blair – Tacanic IPA – President & CEO

Then we need to be careful there.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Is it the rules or the guidance?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

The guidance indicates.

Deven McGraw - Center for Democracy & Technology – Director

Guidance.

Joy Pritts – ONC – Chief Privacy Officer

The guidance has been in effect for about ten years now, so it's pretty kind of rolled into the rule.

John Blair – Tacanic IPA – President & CEO

Then you probably shouldn't use conduit then.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

If you don't have business associate agreements in place, then there would be no way to enforce their adherence to these requirements either.

Deven McGraw - Center for Democracy & Technology – Director

Well, it's not the only way to get them to enforce those requirements, but it is one. Kathleen is right. It is one vehicle for enforcement. Some of what I distributed in this lengthy document that I gave you does raise the issue of sort of what are the tools in HHS's tool shed for enforcing a set of requirements like identification and authentication and encryption and acknowledging that some of them are in the security rule. But to the extent that they're not, and we're talking about conduits that aren't covered by BA's, you know, the other tools that HHS potentially has are through the funding mechanisms that enforce meaningful use and stage HIE grants. But it's not necessarily going to get to everybody.

John Blair – Tacanip IPA – President & CEO

Conduit is already an entity out there. I mean, it's already considered. We probably should pick a different term for now.

Joyce DuBow – AARP Public Policy Institute – Associate Director

Exchange facilitator.

Adam Green – Progressive Chain Campaign Committee – Cofounder

Before you go any further, let me tell you what the guidance actually kind of defines a conduit as. The guidance says the conduit transports information, but does not access it, other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Then that is the right word.

Gayle Harrell – Florida – Former State Legislator

That is the right word. It works.

Joyce DuBow – AARP Public Policy Institute – Associate Director

Yes, but we could just use it, then there's no ability to use the business associate mechanism for enforcement.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

There's another....

Deven McGraw - Center for Democracy & Technology – Director

Hold on. We need one person talking at a time. I heard John Houston.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

No, it's not me.

Deven McGraw - Center for Democracy & Technology – Director

Who did I hear? Sorry.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

It must have been me.

Deven McGraw - Center for Democracy & Technology – Director

Go for it.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

I was going to say there's another way to do that is to talk about....

Deven McGraw - Center for Democracy & Technology – Director

This is Mike, right?

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Right, Mike DeCarlo.

Deven McGraw - Center for Democracy & Technology – Director

Thank you, Mike.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

Those of you who have been working on your comments to the certification program, that's another way to get at it. You wouldn't permit, you know, a certified, if we get to the point of certified systems. You wouldn't permit a certified exchange unless the conduit was also part of that in a certified system and adhered to these requirements. So you could get to it that way.

Paul Eggerman – eScription – CEO

Yes, but that assumes that all the participants have certified systems, certified, certification....

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

You're not. If we're doing this in the context of what OCR and OCN has needs for the Medicare incentive program, then you're not doing that unless you're using....

Joyce DuBow – AARP Public Policy Institute – Associate Director

Yes, I'd rather make it broader.

Gayle Harrell – Florida – Former State Legislator

I think there are other programs or other entities using HIEs that are not, may not be part of the CMS program with certified products.

Deven McGraw - Center for Democracy & Technology – Director

Yes. I think, at this stage, the most that we can do is tee up as an issue enforcing the requirements that we want to see put in place.

Joyce DuBow – AARP Public Policy Institute – Associate Director

And not calling it a conduit would be a good way to start.

Joy Pritts – ONC – Chief Privacy Officer

Is that a recommendation coming out?

Deven McGraw - Center for Democracy & Technology – Director

Yes, it is.

Joy Pritts – ONC – Chief Privacy Officer

Can somebody read it back to me because my notes on this are really kind of all over the place?

Deven McGraw - Center for Democracy & Technology – Director

Essentially what I thought I heard is that folks want to make sure that these criteria that are the conditions under which we get some comfort level in saying that there wouldn't be additional patient consent for rather than having to repeat it, I think we're all on the same page, is getting those effectively enforced, and that the business associate agreement isn't necessarily going to work if the entity that helps facilitate that transaction, our bus driver, is determined, you know, falls into the category of a conduit. And even one could say, and I put that even if the business associate rule did apply, if you have sort of chains of agreements where it's not just one entity providing the service, but multiple entities providing the bus driving services, there's a limited ability for the BA rules to capture that, is my understanding. The funding conditions are another way to enforce, but those are going to have some gaps because not everybody is going to be part of that circle, and this is something that needs to be addressed. And maybe we need something from Congress, but that may be going one step too far.

Joy Pritts – ONC – Chief Privacy Officer

Back to your recommendation, can you roll it up to be a global recommendation?

Deven McGraw - Center for Democracy & Technology – Director

Yes, that, well, one could call it. John Houston, unless I misunderstand your governance point, this is usually where you chime in is that somebody needs to be. Who is responsible for enforcing all this?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Thank you.

Deven McGraw - Center for Democracy & Technology – Director

The governance, and is it all a federal responsibility or is there some role for the states to play as well, which is always Rachel's point.

Joy Pritts – ONC – Chief Privacy Officer

I understand that, but I think that it's not just....

Deven McGraw - Center for Democracy & Technology – Director

What are you hinting at? What are you looking for?

Joy Pritts – ONC – Chief Privacy Officer

We're not just talking about who's going to enforce it if you don't have the rules, right? I mean, are you saying that you need the rules, or are you saying you need to enforce what rules there are?

Deven McGraw - Center for Democracy & Technology – Director

I think we need the rules. I thought we covered that we would need that to get comfortable, and I'm....

Joy Pritts – ONC – Chief Privacy Officer

All right, going back to ... and you're saying that the BA rules are not sufficient and that the what is not sufficient? The certification criteria because they're not broad enough.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

This is Kathleen. I really would like to see that any contractors to a business association with also be a business associate, and that they could not do more than what was allowed under the original covered entity business associate agreement and use that as a way to insure that all intermediaries in an exchange will adhere to what was required in the first place by this covered entity.

Paul Eggerman – eScription – CEO

This is Paul. That sounds fine, but suppose your contractor is like Verizon or Comcast. They're not going to sign a business associate agreement with you.

Deven McGraw - Center for Democracy & Technology – Director

Yes. That's the power differential that I referred to in my document.

Joy Pritts – ONC – Chief Privacy Officer

I'm not sure that that's true. We can talk about it offline, but there are a lot of carriers of different sorts that do have business associate agreements.

Deven McGraw - Center for Democracy & Technology – Director

No, they do, but this point about who decides the terms of those agreements.

Joy Pritts – ONC – Chief Privacy Officer

That I agree with you. That should be part of the picture as well. It's how to ensure that the power of the agreement stays with the initiating covered entity.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

One ... against Verizon has no....

Joy Pritts – ONC – Chief Privacy Officer

Is your recommendation on this one is that the covered entity should what, should dictate the terms of the BA agreement?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

They really should.

John Blair – Tacanic IPA – President & CEO

Yes.

Gayle Harrell – Florida – Former State Legislator

Yes.

Joyce DuBow – AARP Public Policy Institute – Associate Director

That's....

Deven McGraw - Center for Democracy & Technology – Director

Well, but I think we have recommendations, and then I think we need to think realistically about whether that's actually going to work in practice.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

It won't, but it....

Paul Eggerman – eScription – CEO

It's not going to work because ... if I'm a business associate, I may deal with 100 different covered entities.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Yes.

Paul Eggerman – eScription – CEO

They're going to dictate 100 different terms.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Right.

Paul Eggerman – eScription – CEO

In the business associate agreements I need to have with 20 different contractors, it's a full employment discussion for attorneys.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Joy Pritts – ONC – Chief Privacy Officer

But how is that different than what the case is today?

Paul Eggerman – eScription – CEO

No, because a covered entity can't dictate the terms that the business associate in turn has to have with its contractors.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

It depends on who has got the strength in the situation.

Joy Pritts – ONC – Chief Privacy Officer

My understanding that the agents of the business associate had to adhere to the covered entity agreement, the business associate agreement, even though that's not really enforceable, but I could be wrong on that.

John Blair – Tacanic IPA – President & CEO

Say that again.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

They have to, but it does get negotiated frequently.

Gayle Harrell – Florida – Former State Legislator

Yes.

Joy Pritts – ONC – Chief Privacy Officer

Right, but I'm saying that this is what's happening today, so how is it impossible if all you're doing is changing the status of the contractor who is downstream from the business associate?

Adam Green – Progressive Chain Campaign Committee – Cofounder

I can clarify that every business associate, if they want to use a subcontractor, in essence, they do have to have an agreement. It's not under current law a true business associate agreement. They have to receive satisfactory assurances, and they will follow the same requirements as a business associate.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

I think most BA, business associates, do pass that downstream.

John Blair – Tacanic IPA – President & CEO

I wouldn't assume that at all.

Deven McGraw - Center for Democracy & Technology – Director

Yes, and I think the other tricky part is that while the HITECH Act did give greater accountability to business associates in terms of them being able to be held accountable by state and federal authorities for failure to comply, that's not going to apply to the subcontractors. That's just going to be a contractual agreement that gets enforced through traditional contract principles.

Joy Pritts – ONC – Chief Privacy Officer

That's why I was suggesting that it would be a helpful thing if those subcontractors also had business associate status.

Deven McGraw - Center for Democracy & Technology – Director

I think we probably can't do that without an act of Congress.

Joyce DuBow – AARP Public Policy Institute – Associate Director

I agree, but I thought we could actually ... Congress. It was a suggestion.

Deven McGraw - Center for Democracy & Technology – Director

Yes. No, it's not – so, but I think if we're going to make a suggestion for that additional authority, as needed, query whether we would bootstrap it into the business associate realm to begin with or whether there might be more effective enforcement mechanisms that we would look to. That's all I'm saying.

Joyce DuBow – AARP Public Policy Institute – Associate Director

I don't see what alternatives we have to what we have today, and that's one of the places that a lot of the data may be being not used according to the covered entity business associate agreement.

Deven McGraw - Center for Democracy & Technology – Director

Joy?

Joy Pritts – ONC – Chief Privacy Officer

I don't know what you want me to say about that.

Gayle Harrell – Florida – Former State Legislator

What's the solution?

Deven McGraw - Center for Democracy & Technology – Director

Yes. All right. We're reaching the end of what has always been a call that goes rapidly, and we do have a couple of recommendations that we've gotten some more clarity on.

Joy Pritts – ONC – Chief Privacy Officer

Can we clarify those before we get off the phone just to make sure?

Deven McGraw - Center for Democracy & Technology – Director

But I would like to do something else too, and that is to say that to do a gut check with the group, I will reclarify what I think are some specific recommendations that we came to on this call. Can I ask the typist to please mute? But I also do want to get some feedback from folks about the sort of overarching statements about the need for more clear policies in this regard and understanding the time limits, but we

would like to be, but making a statement that, one, it's needed. And, two, we'd like to be as helpful as can possibly be given the structure at drilling down on some of those. What everyone typing and muted?

Gayle Harrell – Florida – Former State Legislator

I'm not sure what you're asking.

Deven McGraw - Center for Democracy & Technology – Director

We drilled down on some very specific issues that we definitely want to put to the policy committee, but there were also some statements in the document that I distributed about the need for overarching policies of which consent is one of them. But I've never gotten an indication that folks didn't feel comfortable with that. But I wanted to make sure that that was the case.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

I never got an indication that people didn't feel comfortable. I'm ... negatives ... Deven....

Deven McGraw - Center for Democracy & Technology – Director

Sorry about that. I was an English major too, so clearly, so I did put some things in recommendations in the document that I sent you that were broader in scope than the more specific ones that we were able to nail down today, which I'll go over in a second that I think we did come to. But I wanted to get a sense of whether folks were comfortable with a recommendation of a need for a drill down on the sort of principles in the national framework that applies to this exchange and the need for the work to begin sooner rather than later, and that we can play an important role, but we understand that the time constraints are big. And we'd like to do this, and the consent is one piece of it, but it's not the only thing, and then we can talk about where we were able to get to specifics. Are folks comfortable with that?

W

Yes.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

I think my answer to that would be yes, but it's going to depend on how far we're drilling down because I think it's obvious from these calls that we can quickly get into the weeds.

Deven McGraw - Center for Democracy & Technology – Director

Yes.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

I think you need to, as the chair, establish a floor below which conversations cannot go.

Deven McGraw - Center for Democracy & Technology – Director

Yes, well, that's fair. It's going to be hard, but it's fair.

Mike DeCarlo – Blue Cross Blue Shield – JD Senior Policy Manager

I'm trying to empower you here, Deven, to cut some stuff off.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

This is Kathleen. I would really like to see you expand on some of your recommendations about governance or some kind of control of what intermediaries who are doing more than just routing the information, what kind of controls could be put in place on their collection, access, use, and disclosure. And I would really like to get to the topic of when do patients expect them to have some control over who can access their data when it is in ... exchange systems.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think that....

Deven McGraw - Center for Democracy & Technology – Director

Hold on, Dixie. There was somebody else in there who started talking.

Judy Faulkner – Epic Systems – Founder

That was Judy, me.

Deven McGraw - Center for Democracy & Technology – Director

Okay, Judy.

Judy Faulkner – Epic Systems – Founder

This is Judy, and I think we need to get to the emergency department scenario because that's where it's most critical to get the information there quickly. The other, which is much more of a referral situation, is of course important too. But I think the emergency department situation is critical.

Gayle Harrell – Florida – Former State Legislator

Yes. Gayle would like to add that I think we really – and ... I'd like to reiterate what Kathleen said and ask, number one, Kathleen, if you could send around the scenario of what you just said earlier.

Deven McGraw - Center for Democracy & Technology – Director

Yes. Kathleen, if you had that language written down. I mean, we do have transcription service, one hopes.

Gayle Harrell – Florida – Former State Legislator

...essential also.

Deven McGraw - Center for Democracy & Technology – Director

And my trusty note taker, but if you wrote that down before the call, please send it.

Gayle Harrell – Florida – Former State Legislator

Yes. Then secondly, I think I'd like to reiterate that I think we need a governance framework for HIEs.

Deven McGraw - Center for Democracy & Technology – Director

Yes. That was one of what I thought was our specific recommendation. The one specific recommendation is the one, which please don't make me articulate it again. I think we've done it several times, and we probably will need to recirculate it to make sure we haven't missed anything, notwithstanding fabulous note taking and transcription. But it involves the one-to-one exchange between physicians for treatment purposes where the bus driver doesn't access individual, identifiable information. We don't think that in that set of circumstances, with the assumptions on certain elements and policies being in place like identification authentication – I thought I wouldn't rearticulate this, and now I'm doing it, but I think you get the gist. That was one.

And then the other one is the need for a way to enforce this for which the BAs, and we would probably need to look into and explore in some more detail. Governance is actually part of the NHIN workgroups purview, quite frankly, but I think it's worth exploring just how well the business associate rules work and don't work in this context. Kathleen is right. It's not a perfect vehicle, but it is one we have available

without getting additional authority, in addition to funding issues. But the governance piece is key, and we can at least make a statement in that regard, I think.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Deven, I think we need to open this up for public comment any moment now. Do you want...?

Deven McGraw - Center for Democracy & Technology – Director

Yes, hold on a second. I just want to make sure we have workgroup feedback, and then we will do that.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Absolutely.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. This is Dixie. What I was going to say is I think, and I would urge us to stay at the same level ... target policy at the level we achieve today, and not get further down in the weeds. And I would also agree with Judy that the emergency room is a good next target.

Deven McGraw - Center for Democracy & Technology – Director

I don't know if it's the next target. I need to do some thinking about that. I think we have a lot of potential targets and limited bandwidth. I think Mike is exactly right, and I need to have some conversations offline with ONC as well as with Rachel, which of course we would vet with you guys, but I don't want to decide this in an ad hoc way.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Deven, on the emergency room, I think it's more that the emergency example is an important one for the query.

Gayle Harrell – Florida – Former State Legislator

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Gayle Harrell – Florida – Former State Legislator

I think it's more the query than the emergency room. It's broader.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Isn't it already allowed under HIPAA for emergency access as one of the capabilities?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

You can break the glass for it.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, but we're talking about exchanges.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Right.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Right. I'm thinking we could extrapolate from there, being a comfort zone for patients.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

But the point is that if you're talking about the emergency room, you're into the query.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Right.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

So we've got to deal with the whole query thing.

Deven McGraw - Center for Democracy & Technology – Director

Right.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Right.

Gayle Harrell – Florida – Former State Legislator

Yes. I think that's the next step is query.

W

Yes.

Gayle Harrell – Florida – Former State Legislator

No. I think, before you even get to query, you need to think about when you ... exchange through just going through an HIE.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

But again, that gets back to that's transport.

Gayle Harrell – Florida – Former State Legislator

No, they can also do retention.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Not necessarily.

Gayle Harrell – Florida – Former State Legislator

And manipulation.

Deven McGraw - Center for Democracy & Technology – Director

Yes, so whether the next use case, and I hate that word, but it's so convenient to use it, is when you actually have an entity in the middle that's doing more than conduit.

John Blair – Tacanic IPA – President & CEO

Right.

Deven McGraw - Center for Democracy & Technology – Director

Or a query example. Again, we want to be responsive to ONC's needs, so we will have some offline discussions about that, but that definitely will be vetted with you guys, and maybe by e-mail.

John Blair – Tacanic IPA – President & CEO

Deven, this is John. One more quick: I think if we can just have a little bit of consensus on some definitions at some point because it sounds like whenever you start to talk about query, it's de facto HIE, and maybe some people would say an HIE could just be a conduit, maybe not, but if we could get that clear.

Deven McGraw - Center for Democracy & Technology – Director

Okay. That's fair.

Joy Pritts – ONC – Chief Privacy Officer

Ultimately that is helpful because it's a factor that will remain constant regardless of what "model" you use.

John Blair – Tacanic IPA – President & CEO

Yes.

Deven McGraw - Center for Democracy & Technology – Director

Right. That's right, Joy. That's a good point. Go ahead, Sarah. Do your magic.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Melissa, are you there? Can we open the phones for public comment?

Operator

Our first question is from Sherry Reynolds with Alliance 4 Health.

Sherry Reynolds – Alliance 4 Health – Executive Director

I have a question and then a real world comment. I didn't transcribe it exactly, but one of your recommendations was that no one other than the original provider or the receiving provider could view the records, and I hope an underlying assumption is that the patients would continue to have full access to their records and that that recommendation wouldn't somehow exclude them.

Deven McGraw - Center for Democracy & Technology – Director

Good point, Sherry. No, absolutely, we were not intending to preempt patient access rights.

Sherry Reynolds – Alliance 4 Health – Executive Director

I knew if you were on the call, Deven, that we'd be fine, but I just wanted it on the record. And the second example is, I live in Seattle, and we sort of already live in the world of EHR integration, and I have a friend who recently went for a second opinion at Swedish Medical Center. And when she returned to her primary care provider at the Poly Clinic, which is a separate nonprofit, the provider questioned her and said I see you went to another physician for a second opinion. Why didn't you ask me first? The patient never authorized that release, but Swedish Hospital subcontracts their EHR to the Poly Clinic, so by default, those two systems are now linked.

Deven McGraw - Center for Democracy & Technology – Director

Wow. Okay. Thanks, Sherry.

Sherry Reynolds – Alliance 4 Health – Executive Director

I'm not giving you a suggestion....

Deven McGraw - Center for Democracy & Technology – Director

Sharing a story, that's appreciated.

Sherry Reynolds – Alliance 4 Health – Executive Director

Was there an intermediary involved? No. Was there a health information exchange involved? No. Was there a conduit? No. It was, by default, their health information system is subcontracted from another provider.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

It's into Judy's example.

Paul Eggerman – eScription – CEO

I think we need to perhaps look at the issue of firewalls and see....

Sherry Reynolds – Alliance 4 Health – Executive Director

Or at least informed consent. I get a lot of questions from women who have abortions, over a million abortions a year. If those records are automatically disclosed to every provider in the system, whether or not we believe they should be for medical reasons is one question, but if it means women are going to opt out of the healthcare system as a result of health information technology, people have pretty big concerns, so I just wanted, you know, as we go through the policy analysis that we continue to refer back to kind of real world examples and the impact on people's lives.

Deven McGraw - Center for Democracy & Technology – Director

Yes. That's a very good point. Thank you. Thanks, Sherry.

Sherry Reynolds – Alliance 4 Health – Executive Director

You're welcome.

Operator

We have no more questions at this time.

Sarah Wattenberg – ONCHIT – Public Health Advisor

I think we can adjourn.

John Blair – Tacanica IPA – President & CEO

Thank you.

Gayle Harrell – Florida – Former State Legislator

Thank you.

W

Thank you very much.

Sarah Wattenberg – ONCHIT – Public Health Advisor

Have a good weekend.

Joy Pritts – ONC – Chief Privacy Officer

Thank you all for your hard work today.

Deven McGraw - Center for Democracy & Technology – Director

Thanks, Joy.

Joy Pritts – ONC – Chief Privacy Officer

Have a good weekend.

Public Comment Received During the Meeting

2. The treatment environment includes many paramedical (unlicensed care givers) that are following treatment orders and do not have a need to know the whole medical history of the patient. The entities are not following 164.514(d)(2)(i) -limit access to need to know--and if the paramedical is in another entity, the "treatment" rule would permit all of the information to flow--which as these records are aggregated, can be a complete life file on an individual.

3. Much of the discussion is focused on providers but the patient also needs to be authorized to access to their own data as well as their child or in some cases family members they are authorized to care for.

4. Whether or not architecture is direct push, federated, centralized at least the following two consent issues are common. Both have major system design considerations... can the patient direct consent to the individual clinician level? Can the patient direct that a portion of their record be excluded from some exchange?

5. Is there a clear policy direction concerning: 1. Can patient direct consent to the individual provider level or to just a provider organization? 2. Can the patient direct consent for a portion of their records based on "content/context"... (diagnosis, type of treatment, type of provider) something that limits access to a "portion" of their records? ... Both of these have a huge affect on architecture and design.

7. Is there a recommendation that identifies: Who "owns" the data...the patient Consumer or if not who? Many existing provider organizations and/or HIE's indicate that they own the data. Could the framework about privacy and security include a statement concerning ownership? Or is it defined somewhere else?